MTR 97B0000084R1

MITRE TECHNICAL REPORT

Intrusion Detection for Air Force Networks

Environment Forecast

October 1997

Leonard J. LaPadula

Sponsor: Air Force
Department: G021

Contract: F19628-C-00001
Project: 03977452OB

Approved for public release; distribution unlimited.

© 1997 The MITRE Corporation

MITRE
Center for Integrated Intelligence Systems
Bedford, Massachusetts

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 1997		**00-10-1997 to 00-10-1997**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intrusion Detection for Air Force Networks. Environment Forecast	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **MITRE Corporation,202 Burlington Road,Bedford,MA,01730-1420**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**23**	

Abstract

Will future intrusion detection tools meet the goals of the US Air Force? To help ensure that they will, the MITRE C2 Protect Mission-Oriented Investigation and Experimentation (MOIE) project is forecasting the environment for Air Force intrusion detection. The forecast should be helpful to commercial interests that may develop capabilities, can be a means of coordinating and shaping future funding decisions, and may provide a common framework for discussing issues.

The first phase of the MOIE project captured customer and corporate experience with intrusion detection tools as well as joint knowledge of the intrusion detection problem. The results are recorded in the paper *Intrusion Detection for Air Force Networks: Operational, Performance, and Implementation Goals*.

The second phase focuses on expected trends over the next several years that might affect the use, design, efficacy, deployment, or maintenance of intrusion detection tools within the Air Force. This paper, a product of the second phase of effort, records trend information developed primarily from in-house technical expertise.

KEYWORDS: intrusion detection, forecast, users, defenders, attackers, technology.

Table of Contents

List of Tables

Section 1

Introduction

The Command and Control (C2) Protect Mission-Oriented Investigation & Experimentation (MOIE) Project, sponsored by the Air Force, develops and promulgates resources to counter information warfare (IW) threats to military C2 computer networks. One component of the threat dimension is exploitative intrusion activity. Even a cursory look at this area reveals that IW attacks are becoming easier to mount, assisted by easily available, user-friendly software and a growing community of cracker web sites and mailing lists.

Given the nature of the C2 mission, the rewards of a successful IW attack on our C2 systems invite the attempt at exploitation. At the same time, we estimate that the number of foreign countries with IW capabilities is increasing rapidly. Since military systems are typically connected to and dependent on public switched networks, they are accessible to an attacker's attempts at exploitation. Moreover, we know from actual investigations performed by AFIWC, ESC, DISA, FIWC, MITRE, and others that many of our C2 systems are vulnerable.

Background

One technological countermeasure to intrusive activity is intrusion detection capability. We expect that current products, although a significant start, will dramatically improve over the next several years, with commercial interests playing a leading role in extending intrusion detection technology. One objective of the C2 Protect Project is to ensure that new products will meet the needs of the Air Force.

The C2 Protect Project has done a two-part forecast of Air Force needs. The first part identified identifies operational, performance, and implementation goals for intrusion detection products. It is available at this web site in the document *Intrusion Detection for Air Force Networks: Operational, Performance, and Implementation Goals*.

The second part of the forecast, contained in this paper, focuses on expected trends over the next several years that might affect the use, design, efficacy, deployment, or maintenance of intrusion detection tools within the Air Force.

Purpose

The results of this task provide an information resource

- to guide vendors developing intrusion detection products

- to assist the Air Force's participation in more global efforts[1]
- to supplement the information used by Air Force mission area teams[2]
- to help planning for acquisition and funding
- to provide a common framework for addressing issues

Approach

We characterize the intrusion detection environment using the following classification as a guide:

- The User Domain
  - Activities: What will they be doing with computers and the information on them?
  - Resources: What will their computing resources be like?
  - Information: What classes, types, and classifications of information will they use?
- The Attacker Domain
  - Interests: What information and computing resources might they target and what will they be trying to do with or to these resources?
  - Tools: What technology supports what they might want to do; what tools might they have or develop?
  - Techniques: What techniques might they use?
  - Trends: What trends might assist crackers?
- The Defender Domain
  - Characterization: What kind of personnel will be called on to play the role of defender and how will they be organized?
  - Responsibilities: What will the nature of the defenders' responsibilities be?
  - Goals: What goals will the defenders have?
  - Frustrations: What do defenders complain about?
- The Technology Domain

---

[1] An example is development of the Automated Intrusion Detection Environment (AIDE) under the DoD Advanced Concept Technology Demonstration program.

[2] Mission area teams, part of the TPIPT (Technical Planning Integrated Product Team) process, identify deficiencies and investigate relevant technology. The TPIPT process marries deficiencies with recommended solution concepts, risk, and cost.

- Networking: What functional and performance changes can we expect in the networking environment?
- Desktop Applications: What will the character of the desktop applications be? Can we expect more distributed processing, more mobile code (e.g., applets, ActiveX, downloadable platform-independent applications, etc.)?
- Server Applications: What will be happening over the next three years in distributed database technology, for example; will it provide more opportunities for attackers or present new challenges?
- Encryption and Authentication: What developments might hinder attackers or cause them to change the character of their attacks?

Presentation of Results

We call the ideas that characterize the intrusion detection environment *trend items*. The next section records the trend items. A trend summary condenses the set of trend items into a major point. Trend summaries characterize each of the four domains shown above. The final section of this paper presents the trend summaries.

Section 2

Trend Items

Each trend item summarizes discussion about a point, principally from the technical meeting held in June (MITRE 1997). Table 1 through Table 4 inclusive display the trend items.

Table 1. Trend Items: Users

Users	
Activities	• Increasing access to external systems with data flow in both directions; it was noted that the distinction between internal and external is beginning to blur • Increased use of fax and email on the Internet • New protocols come into use frequently and users want to take advantage of them; RealAudio is one example • Roving Internet and home-Intranet[3] access • Collaborative computing employing video and audio in addition to textual data may increase; increasing use of video and audio over networks may have a performance impact on intrusion detection tools • Increased use of server applications (for example, as part of a distributed database capability) is probable • Increased use of encryption for signing authored products and to enforce nonrepudiation

[3] By "home-Intranet" we mean the Intranet of the user's organization that the user's computer attaches to.

Users	
Resources	• Faster computers and networking (e.g., 266 MHz and greater Pentiums, Pentium successors, ATM, gigabit Ethernet) • Increasing connectivity via wireless communications • Increasing use of server-capable platforms as desktop computers (for example, Windows NT) • Movement toward Windows NT as the preferred environment for server applications • More hardware and software capabilities to enable portable and transportable computing (e.g., built-in routers) • Increasing use of digital cameras, microphones, and speakers; does this provide new attack opportunities?
Information	• Increasing amounts of temporally critical data[4]; this may mean that denial-of-service attacks will increase • Increasing amounts and kinds of information and security data (e.g., keys, certificates, and passwords) are stored and processed on computers, which are usually connected to at least one network • There will be a desire and push toward multilevel security likely implemented by employing a layered security perimeter with authorized access to computers based on authentication of users

[4] It may be that temporal criticality of data is higher at the lower echelon levels in a military hierarchy. For example, data relating to strategic planning is more likely to be sensitive in a secrecy sense than targeting data transmitted to a mortar battery. Conversely, digitally transmitted targeting data is temporally critical (a transmission service outage of less than a minute could prove fatal) while strategic planning data is not (transmission service outages of minutes or hours are likely not to matter).

Table 2. Trend Items: Attackers

Attackers	
Interests	• With increasing use of various encryption techniques, the keys to encrypted data may become interesting targets • Recently registered systems may be attractive targets on the assumption that the system will initially be poorly configured for security protection • Attackers will likely be interested in any new protocols as fertile ground for exploitation of bugs
Tools	• Data mining and aggregation is becoming more feasible with new tools: this may increase an attacker's capability to get very useful information out of a large set of relatively innocuous attacks • Two kinds (at least) of tools are the broad (e.g., SATAN) and the narrow (specific point-of-attack) tools. Increasing use of distributed, transportable, and portable applications and code may provide more opportunities for the narrow tools—for example, an ordinary NFS mount command can exploit an administrator's bad judgment • Attackers can easily access and use information resources about attack methods and tools provided by other attackers
Techniques	• Install "backdoor" entries to systems during peacetime to be activated during a crisis • Install "dual accounts" to "drain" information • Harness excess CPU power to crack password files • Launch spatially distributed but coordinated attacks

Attackers	
Trends	• Some attacks are becoming stealthy (for example, sending a packet pretending that the connection already exists) • Software increasingly is released with bugs, in usable but possibly insecure condition; does this provide an opportunity for attackers through exploitation of the bugs? • Attackers appear to be increasingly making available information resources about attack methods and tools; thus, an attack that succeeds may rapidly be repeated by other attackers around the world • Attackers' tools appear to be increasing in capability and ease-of-use; thus, even a novice or dabbler may be able, with better tools, to cause significant damage

Table 3. Trend Items: Defenders

Defenders	
Profile	Wide range of responsible personnel, from the very knowledgeable, both legally and technically, to the inexperienced, overwhelmed administrator
Organization	Overlapping authority domains may hinder intrusion detection (e.g., a weather system may be in two different mission domains because it serves both missions, while it may be in a third owning authority domain)
Responsibilities	• Configure and operate a reaction hierarchy • Review the configuration of newly installed computers to ensure that an optimal configuration for protecting against intrusion has been implemented • Manage the instantiation of intrusion detection policy

Defenders	
Goals	• The defenders generally are operating under the new DoD policy of risk management rather than risk avoidance • The defenders often must consider the goal of criminal prosecution • Defenders with deployed forces and mission-oriented sites must be ready to operate in real time under warfare conditions • Defenders at higher-level correlation and analysis sites will need to adapt their operation to warfare conditions. What that adaptation is depends on the CONOP, which we currently do not know. However, we can hypothesize that the activity would be more real-time operation and analysis than long-term historical analysis.
Frustrations	Defenders complain about • User interfaces for tools • Too much data collected by tools • Not enough analysis capability in tools

Table 4. Trend Items: Technology

Technology	
Networking	• More spatially distributed paths: source routing, traffic diversion, end-point moving from one wireless cell to another • Wireless networking will increase, possibly through use of a proxy • Increasing bandwidth over networks will raise a feasibility issue for architectures in which every packet is examined. For example, it may be possible for each host on a very high bandwidth Ethernet to examine just the header of every packet to determine its destination address, but it may be prohibitively expensive to provide a computer that can look at the entirety of every packet in real time. • More and more service oriented as new protocols are demanded and developed • Encrypted tunneling (often referred to as "virtual private network") increasingly used with the desktop or host system as one endpoint, so that intrusion detection techniques that depend on "looking" inside the packet will be pushed into the desktop or host system • Internet Protocol (IP) Version 6 (V6) (IPV6) will provide an Authentication Header[5] (AH) and an Encapsulating Security Payload Header[6] (ESPH); the AH will work against intruders while the ESPH will make it impossible for an ID tool to look inside the encrypted data • Increasing use of ATM: the ATM architecture has implications for placement of intrusion detection since IP packets must be reconstructed from ATM cells before they can be examined[7]

[5] The Authentication Header provides strong integrity and authentication: ensures data is transmitted without undetected alteration, and data received is the same as data sent and claimed sender is the actual sender. (Stevens 1995)

[6] The Encapsulating Security Payload Header (ESPH) provides integrity, authentication, and confidentiality for IP datagrams: in tunnel mode the entire IP datagram is encapsulated within an ESPH; in transport mode the upper-layer protocol data is encapsulated within an ESPH. (Stevens 1995)

[7] The ATM packet is 53 octets in size; thus, in general an IP packet will be transmitted as a set of ATM packets, not all of which will necessarily travel on the same physical path. Thus, ID monitoring of IP packets must be sited to ensure that all ATM cells of an IP packet can be captured. The siting of the ID monitoring must also take into account that reconstruction of an IP packet from ATM cells consumes significant processing power;

Technology	
Desktop Apps	• Increased distributed processing • Network and system management applications becoming web-based (Wallace 1997)
Server Apps	• Federated database technology and use appears to be gaining momentum (e.g., planned AFCERT database) • More distributed (virtual) databases
Encryption	Increased use on network connections; this tends to move the detection problem closer to and, in the case of some encrypted tunneling (AKA virtual private network) even inside the host machines; also, encryption of data could be used by an attacker to make attacks invisible to a detection tool.
Authentication	Availability of public key certificates, smartcards, and hand-held and virtual tokens may increase use of authentication; this may allow intrusion detection tools to cut down on the amount of data they collect, if they can ignore authenticated transmissions.
Intelligent Agents	Intelligent-agent technology holds promise of smarter, real-time capture with potential to enable detection of distributed attacks.
Data Mining	A rapidly developing technology that might assist in predicting attacks by noticing precondition-events in audit logs, recognizing attacks that are in progress, and finding attacks in activity histories.
Knowledge Management	An emerging technology that might assist collaborative assessment of developing intrusion threats: an example is a Collaborative Filter/Recommender system that enables users to annotate events, thereby providing a basis for recommending event sequences for attention.
Search Engines	Web-based search engine technology improving to the point where it might be useful for finding special classes of events relevant to intrusion attempts.

thus, either the ID monitor must be very capable or must be situated "behind" a packet-reconstruction capability (for example, at an end-point of the ATM communications path).

Section 3

Trend Summaries

Each trend summary is a recapitulation of the trend items for one part of the intrusion detection environment. Table 5 displays the trend summaries.

Table 5. Trend Summaries

Domain	Trend Summary
Users	Users will be placing an increasing load on the networks they use and increasing numbers of users will be mobile. Their personal computers will be faster and more capable, more transportable and mobile, including wireless connectivity. They will deal increasingly with temporally critical data, massive volumes of data, and security data (keys, certificates, and passwords). In general, the normal data target for attackers is getting bigger and more interesting; security data as a specialized target is also growing
Attackers	Attackers will likely target security information (keys, passwords) as its use increases. Data mining and aggregation technology will assist attackers. New-release software is likely to be targeted. Applications that require configuring by an administrator (e.g., distributed applications) will provide targets for specific-attack tools. The same capabilities that will increase users' mobility and computing power will also assist the attacker in mounting stealthier, broader, coordinated attacks.
Defenders	Defenders will continue to exhibit a wide spectrum of experience (very knowledgeable to rank novice). They will be operating under the DoD risk management philosophy as opposed to a risk avoidance strategy. Increasingly, they will need capabilities that are usable in wartime. Besides providing protection of operations, they will be concerned with gathering evidence for criminal prosecution. They will need tools that have outstanding human interfaces, that manage collected data effectively, and that have excellent analysis capabilities.

Domain	Trend Summary
Technology	Wireless connectivity, spatially distributed paths, and bandwidth for networks will all increase. More distributed processing and web-based applications will come into use. Users will employ more encrypted network connections and encryption for authentication. A variety of data mining and knowledge management tools and techniques may provide improved capability to find, predict, and assess intrusion attempts.

List of References

LaPadula, L. J., October 1997, *Intrusion Detection for Air Force Networks: Operational, Performance, and Implementation Goals*, The MITRE Corporation, Bedford, Massachusetts.

MITRE, June 19, 1997, Technical Mini-Conference on *Future Trends That May Impact Intrusion Detection*, Arranged by L. J. LaPadula, Attendees: M. J. Gosselin, S. J. Aguirre, F. N. Chase, P. E. Heinle, W. H. Hill, III, M. L. Sheppard, V Swarup, The MITRE Corporation, Bedford, Massachusetts.

Stevens, W. R., 1995, *IP Version 6: An Introduction*, handout at Professional Development Seminar *IP Version 6*, September, 1995, Greater Boston Chapter of the Association of Computing Machinery.

Wallace, S. D., June 1997, *Web-based Management Technology*, MITRE Technical Report 97B0000010, The MITRE Corporation, Bedford, Massachusetts, not in the public domain.

Glossary

AFCERT	Air Force Computer Emergency Response Team
AFIWC	Air Force Information Warfare Center
AH	Authentication Header
ATM	Asynchronous Transfer Mode[8]
C2	Command and Control
CONOP	Concept of Operation
CPU	Central Processing Unit
DISA	Defense Information Systems Agency
DoD	Department of Defense
ESC	Electronic Systems Center
ESPH	Encapsulating Security Payload Header
FIWC	Fleet Information Warfare Center
IW	Information Warfare
MOIE	Mission-Oriented Investigation & Experimentation
NFS	Network File System
SATAN	Security Administrator Tool for Analyzing Networks
VPN	Virtual Private Network

[8] ATM provides data & video multimedia transmissions for local to wide area nets in the 1.5 to 155 Mbps range, at OSI layer < 2.